

AMENAZAS EN INTERNET



Hace unos años, la amenaza más importante a la que se enfrentaban los ordenadores eran los **virus**, a los que posteriormente se sumaron los **gusanos** y los **troyanos**. En la actualidad, a estos tres tipos de software dañino hay que añadir otros programas, documentos o mensajes susceptibles de causar perjuicios a los usuarios de sistemas informáticos. Este tipo de software se denomina **malware**, y bajo él se engloban el **spam**, **spyware**, **adware**, las bromas de mal gusto, etc.

La descarga de archivos de Internet es hoy una práctica muy habitual que, si no se realiza con las debidas precauciones, puede conllevar ciertos peligros. El principal riesgo al efectuar una descarga desde Internet es que el archivo en cuestión pueda contener un virus informático. El peligro aumenta con las descargas desde aplicaciones P2P (**peer to peer**), ya que existe un gran número de virus que se ocultan en ficheros con atractivos nombres, para atraer la atención de los usuarios y conseguir que los descarguen y ejecuten, lo que provocará la infección del sistema.

En la práctica, aunque la descarga de un archivo se haya desarrollado con normalidad y el usuario pueda estar empleando su nuevo programa sin ningún problema, el equipo puede haber sido afectado por algún código malicioso. Estos códigos pueden ser desde **troyanos**, diseñados para robar datos o crear puertas traseras en los ordenadores, hasta **malware** o programas diseñados para hacer daño.

La primera norma básica para descargar archivos de forma segura desde Internet viene de la mano de la prudencia. Existen multitud de páginas "**poco recomendables**" que ofrecen a los navegantes la posibilidad de descargarse aplicaciones, de origen dudoso y que, a menudo, se encuentran infectadas por algún virus. Por ello, lo más conveniente es **evitar cualquier descarga desde este tipo de páginas**.

Debe prestarse atención al **tamaño de los archivos** descargados, sobre todo a través de redes **P2P**. Normalmente, los archivos que, en realidad, son virus camuflados, suelen tener un tamaño muy pequeño, que en absoluto se corresponde con el del archivo que aparentemente ha sido descargado.

También hay que controlar las **extensiones de los archivos** que nos descargamos de la red. El sistema operativo Windows, cuando se instala con la configuración por defecto, oculta las extensiones de los archivos. Quizá Microsoft considera que esta es una información superflua para el usuario común. Pero mantener las extensiones ocultas proporciona una posibilidad de ataque a los autores de **malware**, que dan a sus nombres aparentemente inocentes como, por ejemplo, **felicidades.pps** y que en realidad se llaman **felicidades.pps.exe** y son, por tanto, archivos ejecutables.

En cualquier caso, la medida más recomendable es contar con un conjunto de programas de protección, actualizado con mucha frecuencia. Sólo de esa manera podremos asegurarnos de que las descargas desde Internet no representan una amenaza para nuestro sistema.

A. PHISHING



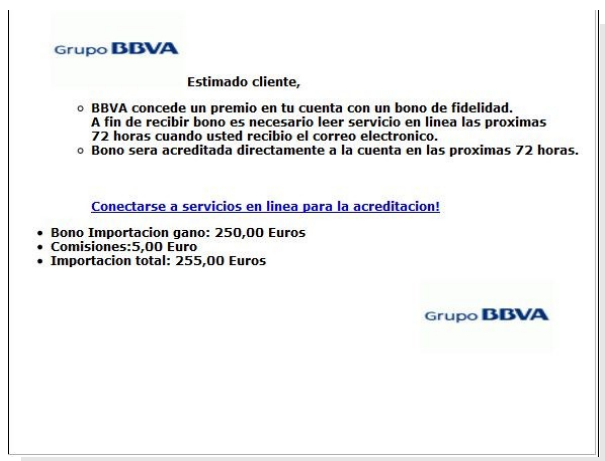
Phishing significa literalmente, 'pescar', 'ir de pesca'. Se trata de un timo en el que el atacante, suplantando la identidad de una empresa de gran implantación, envía correos masivos pidiendo datos confidenciales.

Muchos receptores de estos mensajes se confían al ser el diseño gráfico de la página muy similar al original y, sin darse cuenta de que están cayendo en una trampa, teclean sus números de cuenta bancaria, de tarjeta de crédito, contraseñas, etc. Cuando se enteran de la verdad ya es demasiado tarde.

La vía de difusión más habitual de este tipos de estafas es el correo electrónico, aunque últimamente se han detectado vías alternativas como el teléfono o el fax. Normalmente, lo que hace el atacante de **phishing** es copiar el diseño de las páginas web de bancos y cajas de ahorro de renombre y, con cualquier excusa técnica, se pide al visitante que introduzca sus datos personales. Una vez que el atacante tiene esos datos, pueden operar con la cuenta, vaciarla o comprar con cargo a ella. Obviamente no hay que contestar jamás, bajo ningún concepto, a un correo que pide esa clase de datos. Las entidades financieras no se cansan de recomendar que no se revelen nunca las claves personales aunque sean pedidas en nombre de tales entidades.

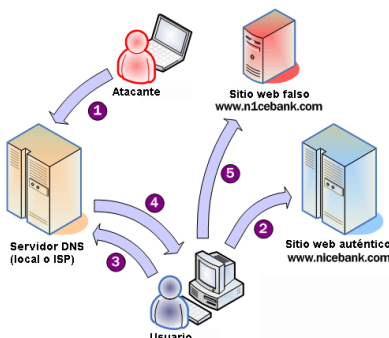
De forma más general, el nombre **phishing** también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un e-mail parecido al oficial,

un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de ingeniería social. Puede verse un ejemplo en luctus.es (en la imagen siguiente)



El término **phishing** fue creado a mediados de los años 90 por los **crackers** que intentaban robar datos en las cuentas de los clientes de **AOL** (*América On Line*). Un atacante se presentaría como empleado de AOL y enviaría un mensaje inmediato a una víctima potencial. El mensaje pediría que la víctima revelara su contraseña con variadas excusas como la verificación de la cuenta o confirmación de la información de la facturación. Una vez que la víctima entregara la contraseña, el atacante podría tener acceso a la cuenta de la víctima y utilizarla para cualquier otro propósito, tales como el **Spamming**.

B. PHARMING



El **pharming** es una nueva modalidad de fraude económico que consiste en suplantar el sistema de resolución de nombres de dominio del servidor **DNS** para conducir al usuario a una página web falsa. El modo de actuar de estos delincuentes consiste en modificar la configuración del protocolo **TCP/IP** o el archivo "**hosts**" del ordenador del cliente, de manera que la víctima acceda a páginas y servidores falsificados pensando que son los auténticos.

Cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una **dirección IP numérica**. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores **DNS** (*Domain Name Server*). En ellos se almacenan tablas con las **direcciones IP** de cada nombre de dominio. A una escala menor, **en cada ordenador** conectado a

Internet hay un fichero en el que se almacena una pequeña tabla con nombres de servidores y **direcciones IP**, de manera que no haga falta acceder a los **DNS** para ciertos nombres de servidor, o incluso para evitarlo.

El **pharming** consiste en modificar este sistema de resolución de nombres, de manera que cuando el usuario cree que está accediendo a su banco o empresa de servicios en Internet, realmente está accediendo a la **IP de una página web falsa**. De este modo, con la técnica del **pharming** se puede atacar a un número de usuarios muchísimo mayor que con la técnica de **phishing** porque no se lleva a cabo a un usuario en un momento concreto, como lo hace el **phishing** mediante sus envíos, ya que la modificación de la tabla de DNS queda almacenada en el servidor, **a la espera** de que un usuario acceda a su servicio bancario. De esta manera, el atacante no está precavido de un ataque puntual, como lo está cuando abre su correo.

El remedio para esta nueva técnica de fraude pasa, de nuevo, por las soluciones de seguridad antivirus. Para llevar a cabo el **pharming** se requiere que alguna aplicación **se instale en el sistema** a atacar (un fichero .exe, un **script**, etc.). La entrada del código en el sistema puede producirse a través de cualquiera de las múltiples vías de entrada de información que hay en un sistema: el correo electrónico (la más frecuente), las descargas por Internet, las copias desde un disco o CD, etc. En todas y cada una de estas entradas de información, el antivirus debe detectar el fichero con el código malicioso y eliminarlo.

Sin embargo, existe un peligro añadido a esta nueva técnica de fraude, que reside en los **servidores proxies anónimos**. Muchos usuarios desean ocultar su identidad (su dirección IP) a la hora de navegar, por lo que utilizan servidores **proxy** instalados en Internet que llevan a cabo la conexión con la IP del servidor en lugar de la IP del cliente. En el peor de los casos, uno de estos servidores **proxy** puede tener la resolución de

nombres alterada, de manera que los usuarios que intenten entrar en su página bancaria - pese a que su sistema local está perfectamente asegurado- sean **redirigidos por el proxy** a una página con el mismo diseño y apariencia de su banco, pero falsa.

C. EL SPAM



El término "**spam**" se utiliza para referirse a **mensajes no solicitados que se reciben en una cuenta de correo electrónico**. El daño que el **spam** provoca puede cuantificarse económicamente en horas de trabajo que se malgastan cada día en todo el mundo, ya no con la tarea de leer los mensajes de **spam**, sino, simplemente, eliminándolos.

Pensemos en una red corporativa con quinientos puestos de trabajo a los que llegan, diariamente, diez mensajes de este tipo. Si debido a estos mensajes se pierden cinco minutos podemos calcular fácilmente el gran número de horas que cada trabajador dedica anualmente al **spam**. Además, si el contenido es lo suficientemente atractivo para que el usuario lea su contenido (o se conecte a alguna dirección de Internet que se indique en el texto) la pérdida de tiempo aumenta exponencialmente.

A los mencionados inconvenientes del **spam** se suman otros peligros añadidos. Aunque no sea lo más habitual, puede contener virus u otros códigos maliciosos o direcciones de Internet que apunten a páginas web que estén preparadas para descargar (de manera no autorizada) algún tipo de programa en el equipo.

El **spam** tiene, generalmente, una serie de características que lo hacen relativamente fácil de identificar. Prácticamente en todos ellos se insta a la compra de algún producto utilizando unas palabras muy similares. De esa manera, un software especializado puede elaborar un determinado perfil del correo recibido para poder catalogarlo como **spam** y eliminarlo antes de que sea descargado en el cliente de correo electrónico, o en los buzones de los usuarios.

Existen sistemas de filtrado de contenidos (que pueden ser fácilmente configurados por el administrador o persona encargada de mantener los equipos informáticos de la empresa) capaces de detectar y borrar el **spam**. Si además el sistema anti-spam está integrado en un software antivirus se neutralizan todos los peligros del **spam**.

D. EL SPYWARE



Se denomina con el término genérico de "**spyware**" a los programas diseñados para **espíar el comportamiento de los usuarios**, fundamentalmente cuando se encuentran conectados a Internet.

El **spyware** son aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, etc. También suelen capturar datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

El **spyware** suele llegar a los ordenadores a través de programas *freeware*, *shareware*, o *demos* de cualquier tipo que, aparentemente, no tienen ninguna peligrosidad. Que una descarga contenga o no **spyware** no depende tanto de si el archivo a descargar es fiable o no, sino de dónde se descarga. De hecho, puede darse el caso de que aplicaciones conocidas y libres de toda sospecha han sido manipuladas para contener un

programa espía. Esta manera de ocultarse en el interior de programas no sospechosos posibilita que se instalen en el PC, al mismo tiempo que el usuario instala la aplicación que acaba de descargar.

La presencia de **spyware** en el sistema supone una agresión a la privacidad de los datos personales que no debe ser consentida. Sin embargo, en la práctica, el **spyware** es uno de los tipos de **malware** más ampliamente distribuido debido a varias razones, propias de la naturaleza de este tipo de aplicaciones, entre las que destacan las siguientes:

- ♦ Utilizan sistemas de camuflaje casi perfectos, ya que normalmente se instalan en el PC junto con algún tipo de aplicación (un cliente de P2P, alguna utilidad para el disco duro, etc.).

- ◆ Los nombres de los archivos que se corresponden con estos programas no suelen dar una idea de su verdadera naturaleza, por lo que pueden pasar desapercibidos entre el resto de ficheros de una aplicación.
- ◆ No provocan ningún efecto visible en el ordenador, ni cuando son instalados, ni cuando se encuentran en plena acción. Por ello, precisamente, los usuarios no suelen preocuparse de si algún programa de este tipo se encuentra instalado en su sistema.

Al no tratarse de virus, ni emplear ninguna rutina que pueda relacionarlos con ellos, los programas antivirus no los detectan. Por tal motivo, para detectar **spyware** es necesario utilizar aplicaciones específicas, como por ejemplo, **Spybot-Search and Destroy**.

Luis González
Profesor de Tecnologías de la Información